Zdrowie Publiczne i Zarządzanie 2012; 10 (B): 191–196
2012, 10 (3): 189–194 doi: 10.4467/20842627OZ.13.020.1168 (online)

Ochrona danych medycznych zawartych w dokumentacji medycznej a wykorzystanie bezpiecznego podpisu elektronicznego

Jolanta Pacian, Anna Pacian, Teresa B. Kulik, Agata Stefanowicz, Hanna Skórzyńska, Dorota Żołnierczuk-Kieliszek, Mariola Janiszewska

Katedra Zdrowia Publicznego Uniwersytetu Medycznego w Lublinie

Adres do korespondencji: Jolanta Pacian, Katedra Zdrowia Publicznego, ul. Chodźki 1, 20-093 Lublin, jolapacian@gmail.com

Abstract

Protection of personal data in health care units

A presentation of the regulations concerning the protection of personal data at health care units is a purpose of the work. Medical data i.e. sensitive data constitute the special category of personal details (sensitive ones) which concern medical condition, information about the genetic code or addictions. A general prohibition on the processing of sensitive data exists, except for the situation, when provisions of the law allow it. In the legal status being in force processing both information referring directly to the medical condition of man, and information the average recipient can acquire these data is forbidden. Processing sensitive personal details without the written consent of the person which they concern, is possible only in the objective of protection of medical condition, providing medical services or curing patients by persons being engaged professionally in curing or with providing other medical services, provided there are created full guarantees of the protection such data. Medical data gathered by the health-service units must be provided with the full legal protection, predicted in the act from 29.08.1997 about the protection of personal data. For creating appropriate conditions of storing medical documentation a manager of the health care unit is held responsible.

Key words: health care units, medical data, protection

Słowa kluczowe: dane medyczne, dokumentacja medyczna, podpis elektroniczny

Ochrona danych osobowych, a szczególnie danych medycznych, stanowi ważny problem w czasach współczesnych. Od tego, w jaki sposób będą chronione nasze dane, zależy poczucie naszego bezpieczeństwa. Im system ochrony jest bardziej stabilny i skuteczny, tym świadomość bezpieczeństwa jest większa. Dlatego tak ważne jest skonstruowanie solidnych podstaw prawnych ochrony danych medycznych. Prawidłowe regulacje prawne zapewnią właściwy obrót tymi danymi i uniemożliwią bezprawne ich udostępnianie. Istotne jest, aby ta ochrona była realizowana zarówno na gruncie konstytucji, jak i innych aktów prawnych rangi ustawy oraz rozporządzeń. Tylko konsekwentne rozwiązania prawne oraz ich egzekwowanie przez podmioty lecznicze, w których takie dane są gromadzone, mogą zapewnić ich należytą ochronę. Celem pracy jest przedstawienie regulacji prawnych dotyczących ochrony danych medycznych zawartych w dokumentacji medycznej oraz zastosowania podpisu elektronicznego w celu zwiększenia bezpieczeństwa ochrony.

Danymi osobowymi są wszelkie informacje dotyczące konkretnej osoby, za pomocą których można tę osobę zidentyfikować, chociaż nie jest ona wyraźnie wskazana. Do danych osobowych zalicza się więc nie tylko imię, nazwisko i adres, ale również dane o cechach fizjologicznych, umysłowych, kulturowych i społecz-

nych. Szczególną kategorię danych osobowych stanowią dane wrażliwe, w tym medyczne. Do tych danych należą informacje na temat: pochodzenia rasowego i etnicznego, poglądów politycznych, przekonań religijnych lub filozoficznych, przynależności wyznaniowej, partyjnej lub związkowej, stanu zdrowia, kodu genetycznego, nałogów, życia seksualnego, skazań, orzeczeń o ukaraniu i mandatów karnych.

Konstytucja RP [1] stanowi gwarancję ochrony danych osobowych, w tym danych medycznych. W art. 51 konstytucji wyrażone zostało prawo do ochrony danych osobowych poprzez to, że nikt nie może być obowiązany inaczej niż na podstawie ustawy do ujawnienia informacji dotyczących jego osoby. Zatem z art. 51, jak słusznie podnoszą J. Barta i R. Markiewicz, „wyprowadzić można prawo każdego do samodzielnego decydowania o ujawnianiu dotyczących go informacji" [2]. Prawo to dotyczy również informacji o danych medycznych. Tak więc każdy ma prawo decydować indywidualnie, czy jego dane mogą być ujawnione. Takie rozwiązanie podkreśla, jak ważna jest ochrona danych osobowych, w tym danych medycznych. Uzależnienie ujawnienia tych danych od woli podmiotu uprawnionego jest wyrazem prawa do samostanowienia o tym, w jakim celu dane będące przedmiotem ochrony zostaną wykorzystane. Co więcej, z art. 51 wynikają trzy prawa: pierwsze do udostępniania, drugie do gromadzenia/przetwarzania i trzecie do zarządzania oraz pozyskiwania przez podmioty służby zdrowia informacji dotyczących danych medycznych.

Podmioty lecznicze tylko w ściśle określonych przypadkach mogą udostępniać chronione dane medyczne. Podmiotami upoważnionymi do wystąpienia z żądaniem udostępnienia danych medycznych zawartych w dokumentacji medycznej są: pacjent lub jego przedstawiciel ustawowy, podmioty udzielające świadczeń zdrowotnych, organy władzy publicznej, NFZ, organy samorządu zawodów medycznych, sądy, prokuratura, minister właściwy do spraw zdrowia, organy rentowe oraz zespoły do spraw orzekania o niepełnosprawności, zakłady ubezpieczeń – za zgodą pacjenta, lekarz, pielęgniarka lub położna. Po śmierci pacjenta prawo wglądu w dokumentację medyczną ma osoba upoważniona przez pacjenta za życia. Natomiast od 1.01.2012 roku do powyższego katalogu uprawnionych do wglądu w dane medyczne, w tym dokumentację medyczną, dołączyły wojewódzkie komisje do spraw orzekania o zdarzeniach medycznych, spadkobiercy w zakresie prowadzonego takiego postępowania, osoby wykonujące świadczenia kontrolne.

Co więcej, dane medyczne zawarte w dokumentacji medycznej mogą być udostępnione przez podmiot udzielający świadczeń zdrowotnych także szkole wyższej lub jednostce badawczo-rozwojowej do wykorzystania w celach naukowych, bez ujawnienia nazwiska i innych danych umożliwiających identyfikację osoby, której dokumentacja dotyczy. Tak szeroki katalog podmiotów uprawnionych świadczy o ogólnej dostępności dokumentacji medycznej.

Z kolei ten tak szeroki dostęp uzasadnia obowiązek zachowania tajemnicy zawodowej. Lekarz, pielęgniarka, położna mają obowiązek zachować w tajemnicy informacje związane pacjentem, a uzyskane w związku z wykonywaniem zawodu. W ten sposób dokumentacja medyczna podlega tajemnicy zawodowej, z uwagi na tego rodzaju dane [3]. Objęcie obowiązkiem tajemnicy zawodowej danych zawartych w dokumentacji medycznej niewątpliwie skutkuje szerokim jej zakresem, ale również stanowi gwarancję, że dane te nie będą bezprawnie wykorzystane. Tak więc krąg uprawnionych, obarczonych obowiązkiem zachowania tajemnicy zawodowej, będzie przestrzegać zasad prawidłowego korzystania z dokumentacji medycznej.

Zgodnie z art. 33 ustawy o ochronie danych osobowych administrator danych musi informować osobę, której dane zostały udostępnione, o prawach, które jej przysługują w zakresie ochrony danych osobowych oraz udzielać informacji o zebranych danych. Wprowadzenie tego obowiązku służy zwiększeniu ochrony nad udostępnianiem takich danych, ponieważ osoba uprawniona posiada pełne informacje o tym, jakie jej dane zostały udostępnione oraz jest świadoma swoich praw i obowiązków w zakresie ochrony danych osobowych. Zatem istnieje mniejsze prawdopodobieństwo, że dane osobowe, w tym dane medyczne, zostaną bezprawnie wykorzystane. Ponadto administrator danych ma obowiązek odmówić udzielenia informacji, jeżeli mogłoby to spowodować ujawnienie wiadomości zawierających informacje niejawne, zagrożenie dla obronności lub bezpieczeństwa państwa, życia lub zdrowia ludzi oraz bezpieczeństwa i porządku publicznego, zagrożenie dla podstawowego interesu gospodarczego lub finansowego państwa, czy też istotne naruszenie dóbr osobistych osób, których dane dotyczą, lub innych osób. Przyznanie administratorowi danych takich kompetencji stanowi gwarancję, że w sytuacjach wyjątkowych, to znaczy gdy istnieje konkretne zagrożenie, dane osobowe nie będą udostępniane z uwagi na występujące ryzyko.

Inny aspekt stanowi udostępnianie danych medycznych przez podmioty lecznicze zakładom ubezpieczeń. Zgodnie z art. 22 ust. 3 ustawy z 22.05.2003 roku o działalności ubezpieczeniowej [4] takie dane mogą być udostępnione dopiero za zgodą ubezpieczonego pacjenta lub osoby, na rzecz której ma zostać zawarta umowa ubezpieczeniowa, albo jej przedstawiciela ustawowego. Z żądaniem przekazania informacji upoważniony jest wystąpić wyłącznie lekarz upoważniony przez zakład ubezpieczeń. Lekarz obowiązany jest do zachowania tajemnicy lekarskiej, a więc do nieudostępniania tych danych innym osobom. Zakres danych obejmuje: informacje o okolicznościach związanych z oceną ryzyka ubezpieczeniowego, z ustaleniem prawa ubezpieczonego do świadczenia, przyczyną śmierci oraz informacje niezbędne do ustalenia prawa osoby zgłaszającej roszczenie do ubezpieczenia. Informacje dotyczące wyników badań genetycznych oraz stanu zdrowia psychicznego nie mogą być udzielane zakładom ubezpieczeń. Te dane należą do danych szczególnie wrażliwych, bardzo łatwo bowiem mogłyby być wykorzystane. Biorąc pod uwagę fakt, że są to dane szczególnie ważne, oraz to, że ich pozyskanie mogłoby być szczególnie cenne dla zakładów ubezpieczeń, taka ochrona jest jak najbardziej wskazana i pożądana.

Podmioty lecznicze gromadzą dane medyczne w postaci dokumentacji medycznej. To właśnie dokumentacja medyczna jest największym zbiorem danych. Dlatego też tak ważne są regulacje prawne traktujące o sposobach i warunkach korzystania z dokumentacji medycznej. Poprzez prawidłową ochronę dokumentacji medycznej realizowana jest również zasada ochrony danych medycznych.

Zgodnie z Rozporządzeniem Ministra Zdrowia z 21.12.2010 roku [5] w sprawie rodzajów i zakresu dokumentacji medycznej oraz sposobu jej przetwarzania dokumentację medyczną dzieli się na indywidualną wewnętrzną – przeznaczoną na potrzeby podmiotu udzielającego świadczeń zdrowotnych oraz zewnętrzną – przeznaczoną na potrzeby pacjenta korzystającego ze świadczeń zdrowotnych. Ponadto wyróżnia się dokumentację zbiorczą dotyczącą ogółu pacjentów lub określonych grup pacjentów korzystających ze świadczeń zdrowotnych i występującą jedynie w podmiotach leczniczych. Dokumentacja medyczna zawiera nie tylko informacje dotyczące przebytych chorób, zabiegów, operacji czy pobytów w szpitalu, ale przede wszystkim dane pacjenta podlegające ochronie na podstawie ustawy z 29.08.1997 roku o ochronie danych osobowych [6]. Tak więc zgodnie z art. 25 ustawy z 06.11.2008 roku o prawach pacjenta i Rzeczniku Praw Pacjenta [7] dokumentacja medyczna zawiera dane dotyczące: oznaczenia pacjenta, oznaczenia podmiotu udzielającego świadczeń zdrowotnych, a także opis stanu zdrowia pacjenta oraz datę jego sporządzenia. Administratorem tych danych jest podmiot leczniczy, który zobowiązany jest do przetwarzania tych danych. Zatem to właśnie podmiot leczniczy jest zobowiązany do przestrzegania wszelkich zasad przetwarzania danych.

Jednym z najistotniejszych obowiązków administratorów danych jest obowiązek zabezpieczenia danych, w szczególności gdy ich przetwarzanie odbywa się w systemach informatycznych [8]. Istnieje ogólny zakaz przetwarzania danych osobowych wrażliwych z wyjątkiem sytuacji, gdy na to zezwalają przepisy prawa. Przetwarzanie oznacza jakiekolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemach informatycznych. Aby zapewnić właściwą ochronę, administrator jest zobowiązany do: zastosowania środków technicznych i organizacyjnych zapewniających ochronę, prowadzenia dokumentacji opisującej sposób przetwarzania danych, wyznaczenia administratora bezpieczeństwa oraz zapewniania kontroli nad tym, jakie dane medyczne były przekazywane.

Artykuł 26 ustawy z 29.08.1997 roku o ochronie danych osobowych wskazuje cztery zasady jakości przetwarzania danych: zasadę legalności, zasadę celowości, zasadę poprawności i adekwatności danych oraz zasadę ograniczenia czasowego przechowywania danych. Zgodnie z pierwszą zasadą dane medyczne muszą być przetwarzane zgodnie z prawem, co oznacza obowiązek przestrzegania również norm prawnych zawartych w innych aktach prawnych, takich jak chociażby Kodeks postępowania karnego. Według zasady celowości dane medyczne mogą być zbierane jedynie do celów oznaczonych i zgodnych z prawem. Zatem w świetle tej ustawy nie jest dopuszczalne dalsze przetwarzanie danych medycznych zebranych niezgodnie z tymi celami. Tak więc administrator danych ujawniający czy udostępniający dane medyczne powinien zachować należytą staranność przy sprawdzaniu, do jakich celów tych danych użyje nabywca.

Natomiast zasada poprawności i adekwatności danych statuuje obowiązek administratora polegający na zapewnieniu, by dane medyczne były merytorycznie poprawne i adekwatne do celów, do których zostały zebrane [9]. Wymaga się od administratora danych systematycznego przeglądu swoich zbiorów danych osobowych. Ponadto dane medyczne przetwarzane przez administratora nie powinny wykraczać swym rodzajem i treścią poza potrzeby wynikające z celu ich przetwarzania. Z zasady ograniczenia czasowego przechowywania danych wynika zaś obowiązek przechowywania danych nie dłużej, niż jest to niezbędne do osiągnięcia celu ich przetwarzania. I tak podmiot udzielający świadczeń zdrowotnych przechowuje dokumentację medyczną, w tym dane medyczne, przez okres 20 lat, licząc od końca roku kalendarzowego, w którym dokonano ostatniego wpisu, z wyjątkiem: dokumentacji medycznej w przypadku zgonu pacjenta na skutek uszkodzenia ciała lub zatrucia, która jest przechowywana przez okres 30 lat, zdjęć rentgenowskich – okres przechowywania 10 lat, skierowań na badania – okres przechowywania 5 lat, dokumentacji medycznej dotyczącej dzieci do ukończenia 2. roku życia, która jest przechowywana przez 22 lata. Po upływie tych okresów podmiot leczniczy niszczy dokumentację medyczną w sposób uniemożliwiający identyfikację pacjenta.

W chwili obecnej rozszerzona została również definicja legalnej zgody osoby, której dane dotyczą, czyli także pacjenta. I tak każda osoba, której dane są przetwarzane, będzie mogła cofnąć wcześniej złożoną zgodę na przetwarzanie tych danych, jeżeli z jakichś powodów uzna, że nie chce, aby jej dane były przetwarzane. Przyznanie kompetencji do cofnięcia zgody na przetwarzanie danych jest wyrazem przyznania przez ustawodawcę osobie, której dane są przetwarzane, prawa do decydowania, w jakim celu jej dane będą przetwarzane. Co więcej, wcześniej złożone oświadczenie woli może być cofnięte, jeżeli zaistnieją pewne okoliczności przemawiające za jego bezzasadnością. Tak więc możliwość cofnięcia wcześniej złożonej zgody jest prawem do samostanowienia każdej osoby o tym, komu jej dane będą przekazywane.

Każda dokumentacja medyczna zawiera dwa rodzaje danych osobowych: (1) dane identyfikujące oraz (2) medyczne. W zależności od rodzaju przetwarzania danych osobowych występują odmienne przesłanki umożliwiające ich przetwarzanie. I tak, jeżeli chodzi o dane identyfikujące, to zgodnie z art. 23 ustawy o ochronie danych osobowych mogą być przetwarzane wówczas, gdy: osoba, której dane dotyczą, wyrazi zgodę, przetwarzanie jest niezbędne do zrealizowania uprawnienia czy obowiązku wynikającego z ustawy, jest konieczne do realizacji umo-

wy lub do wypełnienia celów realizowanych przez administratora. Natomiast w art. 27 powyższej ustawy został wprowadzony zakaz przetwarzania danych wrażliwych, który jednak nie jest zakazem bezwzględnym. O ile bowiem nie można przetwarzać danych ujawniających pochodzenie rasowe czy etniczne, poglądy polityczne, dane o stanie zdrowia, o tyle można te dane rozpowszechniać, gdy m.in. osoba uprawniona wyrazi na to zgodę lub przetwarzanie jest prowadzone w celu ochrony stanu zdrowia, świadczenia usług medycznych lub leczenia pacjentów oraz zarządzania udzielaniem usług medycznych. Dane sensytywne mogą być przetwarzane wyłącznie przez osoby trudniące się zawodowo leczeniem lub świadczeniem usług medycznych. Krąg podmiotów uprawnionych dotyczy zarówno lekarzy, pielęgniarek, położnych, rehabilitantów, techników medycznych, laborantów, jak i aptekarzy oraz farmaceutów [10].

Jeżeli chodzi o pozyskiwanie danych medycznych i zarządzanie [11] udzielaniem usług medycznych, to przez podmioty kompetentne należy rozumieć Narodowy Fundusz Zdrowia oraz wszelkie czynności związane z rejestracją pacjentów [12]. Zwłaszcza podczas rejestracji może dochodzić do przetwarzania danych wrażliwych, znajdujących się w historiach zdrowia i choroby, skierowaniach czy karcie pacjenta. Dlatego też tak ważne jest, aby te dane były należycie chronione przed dostępem osób nieupoważnionych. Pozyskanie tych danych podczas ich przetwarzania przez osoby nieuprawnione mogłoby spowodować szybkie rozpowszechnienie tych informacji. Szczególnie niebezpieczne może być pozyskanie danych dotyczących kodu genetycznego czy różnych zakażeń, takich jak chociażby wirusem HIV. Wykorzystanie tych danych przez osoby nieprzychylne mogłoby narazić osobę, której te dane dotyczą, na wiele cierpień psychicznych, a co za tym idzie naruszyć jej dobra osobiste. Dlatego też te dane powinny być objęte szczególną ochroną na gruncie prawa.

Dodatkowo art. 51 ust. 3 i 4 konstytucji stanowi o prawie sprawowania kontroli nad informacjami o osobie. Taka regulacja ma zapewne na celu wzmożenie ochrony prawnej, jak również monitorowanie celów, w których były udostępniane dane medyczne. Ponadto przepisy te przyznają prawo każdemu do żądania sprostowania oraz usunięcia informacji nieprawdziwych, jak i dostęp do urzędowych dokumentów i urzędowych zbiorów danych. Tak więc Konstytucja RP stoi na straży ochrony danych medycznych oraz dostępu do nich. Poprzez ustawowe ograniczenia ustawodawca realizuje swój główny cel, jakim jest konstytucyjne prawo do ochrony danych medycznych.

Z art. 30 konstytucji wynika prawo do ochrony danych medycznych, które należy interpretować rozszerzająco, a wszelkie wyjątki traktować należy zawężająco [13]. Prawo to doprecyzowuje art. 31 ust. 3 konstytucji, który wymienia dopuszczalne przesłanki ograniczeń w zakresie korzystania z praw i wolności; takim prawem jest także prawo do ochrony danych medycznych [14].

Również z przepisów kodeksu cywilnego wynika obowiązek ochrony danych medycznych. Konstrukcją cywilnoprawną najbliższą instytucji ochrony danych medycznych wydaje się konstrukcja ochrony dóbr osobistych, zawarta w art. 23 i 24 k.c. w związku z art. 448 k.c. Dane medyczne należą do dóbr osobistych, takich jak zdrowie, wolność czy wizerunek, i dlatego powinny być szczególnie chronione. W sytuacji naruszenia pacjent może zgodnie z art. 24 k.c. domagać się dopełnienia czynności potrzebnych do usunięcia skutków naruszenia, poprzez złożenie odpowiedniego oświadczenia i w odpowiedniej formie. Dodatkowo na gruncie art. 448 k.c. może dochodzić zadośćuczynienia pieniężnego lub zapłaty odpowiedniej sumy pieniężnej na wskazany cel społeczny.

Dlatego też prawidłowe zabezpieczenie dokumentacji medycznej poprzez prowadzenie jej w formie elektronicznej i opatrzenie bezpiecznym podpisem elektronicznym stanowi gwarancję ochrony wszystkich danych medycznych. Mimo powszechnej niechęci i braku wiedzy dokumentacja elektroniczna jest bezpieczna, gdyż jej kwestie reguluje rozporządzenie [15], a więc posiada podstawy prawne i związane z nią sankcje nakładane na pracowników za nieprzestrzeganie prawidłowości jej prowadzenia. Prowadzenie dokumentacji w formie elektronicznej wiąże się z zastosowaniem podpisu elektronicznego [16]. Rozporządzenie wyróżnia dwa rodzaje podpisu: podpis opatrzony certyfikatem kwalifikowanym, czyli tzw. podpis bezpieczny, oraz podpis niekwalifikowany, który jest podpisem bezpłatnym, jednak nieposiadającym certyfikatu, który wystawia podmiot uprawniony. Ustawodawca nie narzuca konieczności wyboru konkretnego rodzaju podpisu, pozostawia to do swobodnego uznania podmiotu leczniczego. Niemniej istnieją sytuacje, w których jedynym możliwym do zastosowania podpisem jest ten opatrzony certyfikatem [17]. Zasadne jednak wydaje się wykorzystywanie w praktyce podpisu kwalifikowanego, mimo poniesienia swego rodzaju kosztów finansowych z tym związanych, za który, w razie nieoczekiwanych zdarzeń losowych lub sytuacji, odpowiedzialność poniesie podmiot uprawniony do wydania tegoż certyfikatu. Jak słusznie zauważa M. Jachowicz [18], złożenie elektronicznego oświadczenia woli asygnowanego podpisem elektronicznym niebędącym bezpiecznym podpisem elektronicznym lub niebędącym podpisem elektronicznym weryfikowanym za pomocą ważnego, kwalifikowanego certyfikatu, nie aktywuje normy przepisu art. 5 ust. 2, jak i art. 6 ust. 1 ustawy z 18.09.2001 roku o podpisie elektronicznym [19]. Bezpieczny podpis elektroniczny weryfikowany za pomocą kwalifikowanego certyfikatu nie tylko zapewnia nienaruszalność danych nim objętych, ale przede wszystkim stanowi dowód tego, że został złożony przez osobę określoną w certyfikacie, co dodatkowo wiąże się z wyłącznym dostępem tej osoby do danych przesyłanych drogą elektroniczną.

Podpis kwalifikowany wymagany jest, jak określa rozporządzenie, w przypadku udostępniania dokumentacji przez podmiot leczniczy na zewnątrz. Usługa ta pozwala oznaczyć dokument elektroniczny wiarygodnym czasem, który według Ustawy o Podpisie Elektronicznym stanowi „datę pewną" w rozumieniu przepisów kodeksu cywilnego [20]. W przypadku tradycyjnych dokumentów czas złożenia podpisu ma znaczenie w większości

umów cywilnoprawnych, dokumentach rozliczeniowych i w różnorodnych transakcjach. Analogiczną rolę odgrywa znacznik czasu, w przypadku gdy mamy do czynienia z elektronicznym obiegiem dokumentów [21].

Wykorzystanie znacznika czasu zapewni, iż dokument istniał w danej chwili i jest on dokumentem pewnym. Wiarygodność jest tym większa, gdyż złożenie na dokumencie znacznika czasu, a co za tym idzie opatrzenie go datą pewną, może być dokonane jedynie przez specjalnie upoważnione do tego podmioty. Nie każdy bowiem, kto wyraża wolę, może opatrzyć dokument znacznikiem czasu. Usługa znakowania czasem dokonywana jest jedynie przez kwalifikowany podmiot świadczący usługi certyfikacyjne, co zapewnia bezpieczeństwo najwyższej jakości [22]. Bezpieczeństwo danych opatrzonych znacznikiem czasu zapewnia art. 7 ust. 2 ustawy o podpisie elektronicznym, który precyzyjnie traktuje o istnieniu skutków prawnych daty pewnej i znakowania czasem, oraz Rozporządzenie Rady Ministrów z 7.08.2002 roku w sprawie określenia warunków technicznych i organizacyjnych dla kwalifikowanych podmiotów świadczących usługi certyfikacyjne, polityk certyfikacji dla kwalifikowanych certyfikatów wydawanych przez te podmioty oraz warunków technicznych dla bezpiecznych urządzeń służących do składania i weryfikacji podpisu elektronicznego. Fakt ten dodatkowo jest poparty przepisami kodeksu cywilnego, który również zawiera stanowisko w tej kwestii. Zasadne jest twierdzenie D. Szostka [23], że znakowanie czasem przez kwalifikowany podmiot świadczący usługi certyfikacyjne wywołuje skutki daty pewnej w rozumieniu art. 81 § 2 i 3 k.c., tj. określa datę, w której istniał poświadczony dokument elektroniczny. Dla wywołania skutków prawnych daty pewnej oraz zaistnienia domniemania z art. 7 ust. 3 ustawy z 18.09.2001 roku o podpisie elektronicznym, że podpis elektroniczny został złożony nie później niż w chwili dokonywania usługi, konieczne jest oznakowanie czasem podpisu elektronicznego przez kwalifikowany podmiot świadczący usługi certyfikacyjne. Ponadto koszty stosowania podpisu opatrzonego certyfikatem kwalifikowanym wydają się niewspółmierne do korzyści, jakie przyniesie jego stosowanie [24]. W działaniach długofalowych skutki podpisu bezpiecznego powinny zniwelować koszty poniesione w tej kwestii. Dodatkowo w przypadku konieczności zachowania szczególnej ostrożności niezbędne wydaje się posiadanie bezpiecznego podpisu.

Podobna sytuacja ma miejsce, jeśli chodzi o dane sensytywne, tzn. zawierające m.in. informacje o kodzie genetycznym. Tego rodzaju informacje są wciąż zbyt słabo chronione, często bowiem dochodzi do nieuprawnionego ich wykorzystywania. Zatem należałoby dodatkowo również zaostrzyć sankcje za ich ujawnianie, wprowadzając nowelizację ustawy, która zawierałaby zmienione przepisy regulujące tę kwestię.

Prowadzenie dokumentacji medycznej w wersji elektronicznej z wykorzystaniem bezpiecznego podpisu elektronicznego opatrzonego certyfikatem kwalifikowanym oznacza wycofanie wersji papierowej dokumentacji medycznej. Zgodnie z art. 78 § 2 k.c. dane w postaci elektronicznej są równoważne pod względem skutków prawnych dokumentom opatrzonym podpisami własnoręcznymi [25]. Dodatkowo znajduje uznanie teza R. Popłońskiego [26], że żaden podmiot nie może odmówić skuteczności prawnej oświadczeniu woli opatrzonemu kwalifikowanym podpisem elektronicznym, dlatego iż jest ono oparte na zrównaniu tego dokumentu z wersją papierową. Jak słusznie zauważa E. Wyrozumska [27], także w postępowaniu sądowym dane w postaci elektronicznej będą traktowane jako środek dowodowy (dowód z dokumentu), co znacznie odciąży zakłady opieki zdrowotnej w zakresie wypożyczania sądom dokumentów w wersji papierowej bądź sporządzania z nich wypisów czy odpisów.

Co więcej, regulacje europejskie nakładają na wszystkie państwa członkowskie obowiązek powszechnego stosowania podpisu elektronicznego, a co za tym idzie całkowitego odejścia od form papierowych. W myśl art. 5 Dyrektywy nr 1999/93/WE bowiem państwa członkowskie muszą zapewnić, by zaawansowane podpisy elektroniczne – oparte na kwalifikowanym certyfikacie i złożone za pomocą bezpiecznego urządzenia służącego do składania podpisu – spełniały wymogi prawne podpisu odręcznego [28]. Tak więc podpis elektroniczny będzie stosowany obowiązkowo w obrocie pomiędzy pacjentami a podmiotami leczniczymi, ponieważ prawo europejskie wymaga zgodności z prawem krajowym regulacji wszystkich państw członkowskich.

Wykorzystanie bezpiecznego podpisu elektronicznego do ochrony danych medycznych zawartych w dokumentacji medycznej jest rozwiązaniem prawidłowym, zapewniającym właściwą ochronę. Zastosowanie bezpiecznego podpisu elektronicznego ze znacznikiem czasu stanowi gwarancję, że wszystkie dane zostaną należycie zabezpieczone przed dostępem osób nieuprawnionych. Dane medyczne z uwagi na swój sensytywny charakter powinny być objęte szczególną ochroną, która zapewni nie tylko bezpieczne ich gromadzenie, ale również przetwarzanie i pozyskiwanie. Tylko szczególne środki bezpieczeństwa i skuteczne regulacje prawne prowadzą do kształtowania w świadomości społeczeństwa przekonania, że dane medyczne są bezpieczne.

Piśmiennictwo:

1. Dz.U. z 1997 r., Nr 78, poz. 483 z późn. zm.
2. Barta J., Markiewicz R., *Ochrona danych osobowych. Komentarz*, Zakamycze, Kraków 2001: 83–84.
3. Zimna T., *Dokumentacja medyczna – udostępnianie informacji*, LexOnline 72395.
4. Dz.U. z 2003 r., Nr 11, poz. 66 z późn. zm.
5. Dz.U. Nr 252, poz. 1697.
6. Dz.U. z 2002 r., Nr 101, poz. 926 z późn. zm.
7. Dz.U. z 2012 r., Nr 230, poz. 159.
8. Kulesza E., *Ochrona danych o stanie zdrowia w świetle ustawodawstwa europejskiego i polskiej ustawy o ochronie danych osobowych*, „Prawo i Medycyna" 2000; 5: 110.
9. Kulesza E., *Tylko to co konieczne*, „Rzeczpospolita" 1.12.1999.
10. Wyrok TK z 19.02.2002 r., U 3/01.
11. Czupryna A., Poździoch S., Ryś A., Włodarczyk W.C. (red.), *Zdrowie Publiczne, wybrane zagadnienia*, Wydawnictwo Medyczne „Vesalius", Kraków 2001: 340.

12. Fortak-Karasińska K., Podciechowska A., *Ochrona danych osobowych w placówkach medycznych*, LexOnline.
13. Redelbach A., *Ochrona tajemnicy zawodowej notariusza w świetle u. o.d.o.*, „Rejent" 2001; 5: 160.
14. Oniszczuk J., *Konstytucja RP w świetle orzecznictwa Trybunału Konstytucyjnego*, Zakamycze, Kraków 2000: 241.
15. Rozporządzenie MZ z 21.12.2010 roku w sprawie rodzaju i zakresu dokumentacji medycznej oraz sposobu jej przetwarzania, Dz.U. Nr 252, poz. 1697.
16. Postanowienie NSA z 10.09.2008 roku, I OZ 673/08 oraz postanowienie SN z 26.03.2009 roku, I KZP 39/08.
17. Jaromin A., *Elektroniczna dokumentacja medyczna pacjentów*, „Menedżer Zdrowia" 2010; 2: 68.
18. Jachowicz M., *E-administracja jako konsekwencja powstania i rozwoju społeczeństwa informacyjnego*, „Casus" 2004; 2: 21.
19. Ustawa z 18.09.2001 roku o podpisie elektronicznym (Dz.U. Nr 130, poz. 1450 z późn. zm.).
20. Kodeks cywilny (Dz.U. 1964 r., Nr 16, poz. 93 z późn. zm.).
21. Polskie Centrum Certyfikacji Elektronicznej, http://www.sigillum.pl/sig-cmsws/page/?F;161 (dostęp:15.03.2011).
22. Znacznik czasu, http://www.laurus.pl/index2.php?option=com_content&do_pdf=1&id=98 (dostęp: 07.04.2011).
23. Szostek D., *Elektroniczna data pewna*, „Przegląd Prawa Handlowego" 2003; 3: 19.
24. Kościelny T., Szaniawski K., *Komentarz do art. 7 ustawy z dnia 18 września 2001 r. o podpisie elektronicznym*, w: Kościelny T., Szaniawski K. (red.), *Ustawa o podpisie elektronicznym. Komentarz*, Zakamycze, Kraków 2003: 102.
25. Kocut W.J., *Charakter prawny podpisu elektronicznego*, „Przegląd Prawa Handlowego" 2002; 4: 36.
26. Popłoński R., *Podpis elektroniczny w prawie cywilnym i administracyjnym*, „Prawo Bankowe" 2003; 12: 25.
27. Wyrozumska E., *Elektroniczne oświadczenia woli w ustawie o podpisie elektronicznym i po nowelizacji kodeksu cywilnego*, „Przegląd Prawa Handlowego" 2003; 8: 45.
28. Jackowski M., *Glosa do postanowienia SN z dnia 26.03.2009 r. I KZP 39/08, teza 4*, „Przegląd Sejmowy" 2010; 2: 166.